

**LEVINE, LAGAPA & BLOCK**

1200 NINETEENTH STREET, NW  
SUITE 602  
WASHINGTON, D.C. 20036  
(202) 223-4980  
FAX (202) 223-0833

DOCKET FILE COPY ORIGINAL

**RECEIVED**

**JAN 14 1994**

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

January 14, 1994

William F. Caton  
Acting Secretary  
Federal Communications Commission  
1919 M Street, N.W.  
Washington, D.C. 20554

Re: Comments In the Matter of Policies and Rules  
Concerning Toll Fraud CC Docket 93-292

Dear Mr. Caton:

In accordance with Sections 1.415 and 1.419 of the Commission's Rules of Practice and Procedure, enclosed please find for filing an original and 9 copies of the comments of Communications Managers Association, New York Clearing House Association, and the Securities Industry Association in the captioned proceeding. Please date stamp and return the additional copy for our files.

Please feel free to me if you have any questions regarding this filing.

Sincerely,



Debra L. Lagapa  
Levine, Lagapa & Block  
1200 Nineteenth Street, N.W.  
Suite 602  
Washington, D.C. 20036

Counsel for Communications  
Managers Association, the New  
York Clearing House Association,  
and the Securities Industry Association

No. of Copies rec'd \_\_\_\_\_  
List ABCDE \_\_\_\_\_

029

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

In the Matter of  
Policies and Rules  
Concerning Toll Fraud

CC Dkt. 93-292

**COMMENTS OF THE  
COMMUNICATIONS MANAGERS ASSOCIATION,  
THE NEW YORK CLEARING HOUSE ASSOCIATION  
AND THE SECURITIES INDUSTRY ASSOCIATION**

Debra L. Lagapa  
LEVINE, LAGAPA & BLOCK  
1200 Nineteenth Street, N.W.  
Suite 602  
Washington, D.C. 20036  
(202) 223-4980

Counsel for the Communications  
Managers Association, the  
New York Clearing House Association,  
and the Securities Industry Association

## TABLE OF CONTENTS

	<u>Page</u>
Summary .....	ii
Background .....	1
Discussion.....	2
I. Commission Action is Urgently Needed to Stem the Proliferation of Telecommunications Fraud.....	2
II. Carriers Must Share In the Responsibility to Prevent and Detect CPE-Based Fraud .....	4
A. A Carrier should be Required to Offer Services that Minimize a Customer's Exposure to CPE-Based Fraud .....	5
B. Existing IXC Fraud Detection Services Do Not Provide Adequate Protection for Most Telecommunications Customers.....	7
III. The Commission Should Amend Part 68 to Make Equipment Vendors More Accountable for CPE-Based Fraud .....	9
Conclusion .....	10

## **SUMMARY**

Phone service theft through the infiltration of a customer's PBX or other CPE is a huge and growing problem in the United States. Given the vast number of entry points and the sophisticated tactics of computer hackers, it is clear that CPE-based fraud can only be controlled through the cooperative efforts of equipment vendors, carriers and customers. Under current law, however, carriers and equipment manufacturers have little or no incentive to assist customers in preventing phone service theft or in minimizing losses once fraud occurs. For this reason, the Communications Managers Association, the New York Clearing House Association and the Securities Industry Association (collectively the "User Parties") urge the Commission to adopt standards that will allocate responsibility for the prevention and detection of CPE-based fraud and equitably apportion the losses attributable to such fraud.

For example, as a precondition to sharing CPE-based fraud losses with their customers, carriers should be required to fully inform customers of the security risks involved in using certain carrier services and to offer, at cost-based rates, a basic package of fraud detection services designed to help users limit their exposure to phone service theft. These services would include customized call blocking features, real-time security reporting, and call monitoring via trunk-based parameters that would signal sudden spikes in call volume, unusual call patterns, or sudden increases in calls to particular area codes or countries. Once such services are in place, toll fraud losses could be

allocated between carriers and customers according to their respective responsibilities.

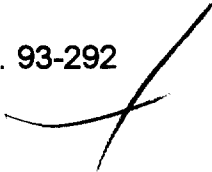
Equipment manufacturers and vendors must also be held accountable for their part in the proliferation of CPE-based toll fraud. As the Commission recommends, equipment manufacturers should be obligated to provide effective warnings concerning the potential toll fraud risks associated with the use of CPE. In addition, the Commission should require, pursuant to its authority to register terminal equipment, that manufacturers build appropriate security measures into their CPE. Customers should be able, for example, to remove, not merely disable, options and features that are particularly vulnerable to fraud and to create multiple levels of security to more effectively limit access to their CPE. Such measures will help to ensure that customers are better able to protect themselves from the unauthorized use of their phone service and equipment.

**RECEIVED****JAN 14 1994**FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

\_\_\_\_\_  
In the Matter of  
Policies and Rules  
Concerning Toll Fraud  
\_\_\_\_\_

CC Dkt. 93-292



**COMMENTS OF THE  
COMMUNICATIONS MANAGERS ASSOCIATION,  
THE NEW YORK CLEARING HOUSE ASSOCIATION  
AND THE SECURITIES INDUSTRY ASSOCIATION**

The Communications Managers Association ("CMA"), the New York Clearing House Association ("NYCHA") and the Securities Industry Association ("SIA") (collectively the "User Parties"), submit these comments in response to the Notice of Proposed Rulemaking issued in the above-captioned proceeding on December 12, 1993.<sup>1</sup>

**BACKGROUND**

The CMA, founded in 1948, is the second oldest telecommunications user group in the nation. Its membership consists of more than 200 of the nation's prominent companies, many of which are members of the Fortune 500. NYCHA is an association of financial institutions whose members include eleven of the leading banks in New York.<sup>2</sup> It serves primarily

<sup>1</sup> *In the Matter of Policies and Rules Concerning Toll Fraud*, CC Dkt. No. 93-292, Notice of Proposed Rulemaking (released Dec. 2, 1993) ("NPRM").

<sup>2</sup> The members of the New York Clearing House Association are The Bank of New York, The Chase Manhattan Bank, N.A., Citibank, N.A., Chemical Bank, Morgan Guaranty Trust Company of New York, Bankers Trust Company, Marine Midland Bank, N.A., United States Trust

as a clearinghouse through which members settle accounts and present checks and other payment instruments. NYCHA also represents its members in regulatory matters on issues of common concern. SIA is a trade association of over 600 securities firms in the United States and Canada. Its members account for approximately 90 percent of the securities business in North America.

The User Parties applaud the Commission for its comprehensive inquiry into the burgeoning problem of telecommunications fraud. As large purchasers of telecommunications services, the User Parties are particularly vulnerable to -- and indeed have already been victimized by -- long distance phone service thieves. The User Parties thus have a direct interest in developing policies that aid in the detection and prevention of all forms of telecommunications fraud and that fairly apportion the liability for toll fraud losses once they occur.

## **DISCUSSION**

### **I. COMMISSION ACTION IS URGENTLY NEEDED TO STEM THE PROLIFERATION OF TELECOMMUNICATIONS FRAUD.**

It has been nearly three years since we first urged the Commission, in the Pacific Mutual proceeding, to adopt specific guidelines to allocate responsibility for the prevention of, and ultimate liability for, losses attributable to phone service theft.<sup>3</sup> While there is increased industry and public

---

Company of New York, National Westminster Bank USA, European American Bank and Republic National Bank of New York.

<sup>3</sup> *In the Matter of Petition for Declaratory Ruling and for the Establishment of Policies Relative to the Allocation of Responsibility for Toll Fraud Abuse Involving Combinations of Remote Access Network Services and Customer Premises Systems*, File No. ENF 91-07, Comments of the Securities Industries Association, VISA U.S.A., Inc., and the New York Clearing House Association (filed Apr. 15, 1991).

awareness of the problem today, the need for Commission action remains urgent. Toll fraud has reached epidemic proportions in the United States. The U.S. Secret Service now estimates that between one to five billion dollars are lost annually due to the theft of telephone service.<sup>4</sup> According to one expert, companies with a typical PBX system "risk a one in 18 chance of being hacked."<sup>5</sup> Average losses are estimated at more than \$60,000 per fraud incident,<sup>6</sup> though it is not uncommon for customers to sustain losses of \$250,000 or more.

Aspiring criminals are continually devising new ways to infiltrate PBXs and other CPE to commit phone service theft. One common means of access has been by "hacking" the password for the Direct Inward System Access ("DISA") feature on the customer's CPE.<sup>7</sup> As users have become more savvy about this particular form of CPE-based fraud<sup>8</sup> -- and have severely restricted or eliminated entirely this calling feature -- telephone hackers have turned increasingly to voice mail systems, call attendant services and remote access maintenance ports as profitable avenues for toll thievery.

---

<sup>4</sup> Karen Lynch, *Carriers Urged to Take Action Against Telephone Fraud*, *CommunicationsWeek*, Dec. 6, 1993 at 11. One expert, the president of a consulting group specializing on toll fraud issues, places the loss figure at closer to \$8 billion annually. Dan O'Shea, *Security Products Abound, But Toll Fraud Is Too Tough*, *Telephony*, Aug. 30, 1993 at 7.

<sup>5</sup> Carl Steffens, *What You Should Know About PBX Security*, *Telecommunications*, Oct. 1993 at 53 (quoting John Haugh, chairman of Telecommunications Advisors, Inc.).

<sup>6</sup> *Id.*

<sup>7</sup> DISA allows company employees to call the office during non-business hours and gain access to a PBX or Centrex system using a password. The employee can then place phone calls over the company's outgoing lines.

<sup>8</sup> For convenience, we will refer to the illegal access and use of a customer's PBX, voice mail system or other CPE as "CPE-based fraud."



Under the present regime, carriers and equipment manufacturers have little or no incentive to assist customers in combating CPE-based fraud, or even to alert them to vulnerabilities in the use of CPE or services. While carriers rely on tariff provisions to hold their customers strictly liable for unauthorized long distance charges, equipment vendors cite limited warranties and other limitations on liability in standard form contracts to absolve themselves of any responsibility.

Accordingly, we renew our request for clear and specific guidelines that will allocate responsibility for the prevention and detection of, and ultimately liability for, losses attributable to toll service theft through the fraudulent use of CPE. The Commission's guidelines should accomplish two goals. First, they should provide incentives for the development and proper use of safeguards by all affected parties, thereby reducing the magnitude of the toll fraud problem. Second, they should spread losses equitably, in a manner that neither penalizes the innocent nor rewards the negligent.<sup>9</sup>

## **II. CARRIERS MUST SHARE IN THE RESPONSIBILITY TO PREVENT AND DETECT CPE-BASED FRAUD.**

As the Commission now recognizes, a carrier's attempt to hold its customers completely responsible for all toll charges resulting from CPE-based fraud is inequitable and unreasonable, especially where the carrier fails to warn users of the security risks inherent in the services that it provides. NPRM at ¶ 24.<sup>10</sup> While the Commission's tentative conclusion is a step in the right

---

<sup>9</sup> Because the User Parties focus their comments on issues relating to CPE-based fraud, they express no views on whether the recommendations they propose to balance the responsibility for the detection, prevention and assumption of losses attributable to CPE-based fraud would be applicable or appropriate to other forms of telecommunications fraud.

<sup>10</sup> The carriers' obligation to inform customers of security risks should be ongoing, reflecting the most current information about emerging fraud scams. In order to ensure that such information is communicated effectively to customers, NPRM at ¶ 24, carriers should be required

direction, it fails to hold carriers fully accountable for their part in preventing unauthorized calls and in minimizing losses once fraud has occurred.

A. A Carrier Should be Required to Offer Services That Minimize a Customer's Exposure to CPE-Based Fraud.

Even when consumers are fully informed of the risks associated with certain attractive CPE features and interexchange services -- and take proper security precautions -- fraud can and will occur. Physical interdiction of trunks is always possible (especially in multi-tenant buildings), and ingenious hackers can quickly develop countermeasures to existing security precautions. In many instances, the defrauded customer, who may be no more culpable than the owner of a stolen car used to rob a bank, is completely unaware that its service is being abused until the first shocking phone bill arrives.

Because they alone possess contemporaneous information regarding traffic patterns and call volumes,<sup>11</sup> interexchange carriers ("IXCs") are in the best position to monitor long distance traffic for signs of fraudulent abuse. As a precondition to shifting liability for unauthorized charges to their customers, the IXCs should be required to offer, at cost-based rates, a package of basic services designed to help users minimize their exposure to phone service theft. As we earlier recommended, these services should include customized call blocking features, real-time security reports, and call monitoring via trunk-based parameters that would signal sudden spikes in call volume, unusual call patterns, or sudden increases in calls to particular area codes or countries.

---

to maintain databases of customer contact names and addresses. In our experience, "Dear Telecom Manager" letters rarely make their way to the right person.

<sup>11</sup> Given that telephone bills generally are received at least 15 days after the close of the monthly billing cycle, a \$5,000 toll fraud incident can quickly -- and without the customer's knowledge -- mushroom into a catastrophic \$200,000 problem.

If a particular parameter is exceeded, the IXC should be required to notify the affected customer within 30 minutes and to provide unrated call detail (either online, by fax or by E-mail) within three hours so that the customer can confirm the presence or absence of fraudulent calling. Finally, the IXCs should be required to help customers reduce their exposure once fraud is detected by offering to restrict calling by area codes or countries, time of day, or other relevant parameters. Customers should not be forced to block all outbound trunks if less restrictive means are technically available to preclude further fraud.

Once such services are made available to consumers, toll fraud losses should be allocated between carriers and customers according to their respective responsibility. Thus, if a carrier failed to provide timely notice that a parameter had been exceeded, it would be liable for the resulting fraud losses. The carrier would also be liable if it failed to provide unrated call detail within the three-hour time period, or if it failed to respond in a timely manner to a customer's report of suspicious calling activity. Conversely, if a customer failed to take steps to mitigate unauthorized use after being notified of usage anomalies, the customer would be responsible for the loss. Similarly, if a customer declines to purchase fraud prevention services after being notified by the carrier of the risks of unauthorized usage, the customer should be liable for any unauthorized calls resulting from CPE-based fraud.<sup>12</sup>

---

<sup>12</sup> In no circumstances, however, should a customer be held responsible for fraud losses resulting from a hacker's infiltration of the carrier's premises or equipment.

**B. Existing IXC Fraud Detection Services Do Not Provide Adequate Protection for Most Telecommunications Customers.**

---

As the Commission notes, the major IXCs have recently introduced fraud prevention services designed to help businesses protect their CPE from telephone hacking. While these programs indicate a willingness on the part of carriers to assist customers when it is profitable for the IXCs to do so, the programs' shortcomings render them of limited utility in the ongoing battle against toll fraud.

First, these fraud prevention services are offered within a legal framework that shields carriers from all liability for unauthorized toll calls. Not surprisingly, therefore, carrier services that shift a portion of the liability to the IXCs themselves, such as AT&T's NetProtect Premium and Advanced programs, are extremely costly, and the circumstances under which the carrier assumes liability are strictly contained. For example, under AT&T's NetProtect Advanced service, customers pay a service establishment charge of \$120 per covered customer telephone system ("CTS") -- *i.e.*, a single PBX or electronic key system -- plus a monthly recurring charge of between \$25-125 per CTS. Even after paying these charges, customers remain liable for the first \$25,000 in unauthorized charges, plus any toll fraud calls that are placed two or more hours after AT&T notifies the customer of the suspected fraud.<sup>13</sup>

Second, customers must often meet minimum usage or term requirements in order to be eligible for existing carrier fraud protection services.

---

<sup>13</sup> SprintGUARD Plus is a somewhat more affordable service, and credits customers for any unauthorized charges stemming from CPE fraud that exceed \$10,000 per incident. Customers remain liable for fraud losses occurring four or more hours after Sprint's notification of possible unauthorized use. The customer is also liable for any fraud losses that occur within a 14-day period from the last fraud incident. MCI does not have a specific liability sharing program, but offers customers private fraud insurance from the National Union Fire Insurance Company. MCI will also give customers a one-time 30 percent reduction on long distance charges attributable to toll fraud.

Under AT&T NetProtect Advanced service, a minimum of 30 percent of a customer's 800 lines must come from AT&T. With AT&T NetProtect Premium, which carries no deductible, 100 percent of the customer's 800 lines must be provided by AT&T. Although Sprint recently eliminated its \$30,000 minimum usage requirement for SprintGUARD Plus, customers must commit to a minimum one year term.<sup>14</sup>

Third, although all three major IXC's provide some monitoring services at relatively modest rates, there is no consequence to the carrier from failing to notify a customer in a timely manner of suspected fraudulent calling.<sup>15</sup> In all circumstances, the customer remains entirely responsible for all long distance charges attributable to phone service theft.<sup>16</sup>

Until the IXC's have a real economic incentive to assist customers in combating CPE-based fraud, they are unlikely to offer and promote truly effective fraud prevention services. As a direct result of federal laws that place a \$50 limit on a calling card customer's liability for fraudulent use,<sup>17</sup> the IXC's and other telephone utilities have stepped up calling card fraud containment efforts, thereby reducing the useful life of a "hot " card from nearly a week to just three hours. In a similar vein, the Commission can facilitate CPE-based fraud containment efforts by ensuring that those parties who are best equipped to

---

<sup>14</sup> *Sprint Expands Fraud Programs*, CommunicationsWeek, Apr. 26, 1993 at 31.

<sup>15</sup> Similarly, there is no consequence to the carrier if it fails to respond in a timely manner to a customer's report of suspicious calling activity.

<sup>16</sup> All carriers whose networks are vulnerable to phone service theft should be required to offer cost-based, real-time monitoring services. While some cellular carriers do make an effort to notify customers of suspected fraudulent activity, others may not (or may do so inconsistently). And while it has been our experience that cellular companies are willing to absorb the losses attributable to cellular fraud, all subscribers ultimately bear a portion of these costs. Thus, the focus must be on greater fraud prevention and containment efforts.

<sup>17</sup> See 12 C.F.R. § 226.12.

prevent, detect and contain long distance phone service theft -- the carriers -- bear some responsibility for toll fraud losses.

**III. THE COMMISSION SHOULD AMEND PART 68  
TO MAKE EQUIPMENT VENDORS MORE ACCOUNTABLE  
FOR CPE-BASED FRAUD.**

---

The User Parties support the Commission's proposal to amend Part 68 to require equipment manufacturers to provide warnings regarding the potential toll fraud risks associated with the use of CPE. NPRM at ¶ 40. Those warnings, as the Commission noted, must be communicated effectively through prominent and conspicuous notices in instruction manuals and other literature accompanying the equipment. In particular, manufacturers should be required to explain fully the use of default passwords and the necessity of modifying them before the CPE is placed into operation. Vendors should further be required to maintain databases of customer contacts so that as new fraud schemes are uncovered, customers can be apprised of additional security risks. As discussed above, however, ensuring customer awareness of CPE vulnerabilities is only part of the solution.

Part 68 is intended to protect the public switched network from "harms caused by the connection of terminal equipment and associated wiring." 47 C.F.R. § 68.1. Pursuant to the FCC's authority to register terminal equipment, 47 C.F.R. § 68.102, the Commission should require manufacturers of PBXs and other CPE to build appropriate security features into all terminal equipment. For example, manufacturers should build into CPE the ability to remove, not merely disable, options and features that are particularly vulnerable to fraudulent use. In addition, multiple levels of security should be provided to more effectively limit access to a customer's CPE.

While the Commission's limited jurisdiction over equipment manufacturers and vendors may preclude it from requiring such entities to assume liability for losses when they fail to act responsibly to detect or prevent fraud occurrences, the measures outlined above will help to ensure that customers are better able to protect themselves from the unauthorized use of CPE.

### **CONCLUSION**

The carriers' view that customers should be solely responsible for losses attributable to phone service theft is inequitable and unreasonable. Equally unconvincing, however, are the claims of some users that interexchange carriers should be strictly liable for all toll fraud losses in all circumstances. Strict liability either direction creates skewed incentives for the prevention and detection of telephone service theft. Users share in the responsibility to safeguard their networks, as do the equipment vendors who supply PBXs and other CPE. Given the vast number of entry points and the sophisticated tactics of computer hackers, it is clear that CPE-based fraud can only be controlled through the cooperative efforts of equipment vendors, carriers and customers. By more equitably apportioning the liability for resulting toll fraud losses, the

Commission will spur the various stakeholders to devise and implement effective measures to detect and curtail CPE-based fraud.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Debra Lagapa". The signature is fluid and cursive, with the first name "Debra" and last name "Lagapa" clearly distinguishable.

Debra L. Lagapa  
LEVINE, LAGAPA & BLOCK  
1200 19th Street, NW, Suite 602  
Washington, D.C. 20036  
(202) 223-4980

Counsel for the Communications  
Managers Association, the  
New York Clearing House Association  
and the Securities Industry Association

100.01 fndcomnt